IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Confirmation No.: 7312
BUER, *et al*	Art Unit: 2437
Appl. No.: 10/728,192	Examiner: Williams, Jeffrey L.
Filed: December 4, 2003	Atty. Docket: 2875.0170001
For: **Tagging Mechanism for Data Path Security Processing**	

Brief on Appeal Under 37 C.F.R. § 41.67

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

A Notice of Appeal from the final rejection of claims 1-7, 9, 13-33, and 35-40 was filed on April 14, 2010. Appellants hereby timely file one copy of this Appeal Brief, together with the required fee set forth in 37 C.F.R. § 41.20(b)(2).

It is not believed that extensions of time are required beyond those that may otherwise be provided for in documents accompanying this paper. However, if additional extensions of time are necessary to prevent abandonment of this application, then such extensions of time are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required therefor (including fees for net addition of claims) are hereby authorized to be charged to our Deposit Account No. 19-0036.

Table of Contents

I. Real Party In Interest

The real party in interest in this Brief on Appeal is Broadcom Corporation ("Broadcom"), having its principal place of business at 3300 California Avenue, Irvine, California, 92617. An assignment assigning all right, title, and interest in and to the patent application from the inventors to Broadcom was recorded in the United States Patent & Trademark Office on March 30, 2004 at Reel 015160, Frame 0383.

II. Related Appeals, Interferences and Other Proceedings

To the best knowledge of Appellants, Appellants' legal representative, and Appellants' assignee, there are no other appeals or interferences which will directly affect or be directly affected or have a bearing on a decision by the Board of Patent Appeals and Interferences ("the Board") in the pending appeal.

III. Status of Claims

The application was originally filed on December 4, 2003 with 53 claims (numbered 1-53). In the Amendment and Reply filed on January 3, 2008, Appellants amended claims 1-7, 9, 13-28, 30-33, and 35-39 and canceled claims 8, 10-12, 34, and 41-53. In the Amendment and Reply filed on September 4, 2008, Appellants further amended claim 7. In the Amendment and Reply filed on July 6, 2009, Appellants amended claims 1, 5, 17, 26, 30, and 37.

The pending claims, claims 1-7, 9, 13-33, and 35-40, were finally rejected in an Office Action mailed on October 14, 2009. In the Notice of Panel Decision from Pre-Appeal Brief Review, the panel maintained the rejection of the pending claims.

IV. Status of Amendments

All amendments have been entered. The Office Action dated October 14, 2009, responded to Appellants' amendment filed July 6, 2009. Thus, claims 1-7, 9, 13-33, and 35-40 are pending. A complete listing of claims and their associated status is included in the Claims Appendix of Section VIII.

V. Summary of Claimed Subject Matter

A. *Background*

The claims on appeal are directed to methods and associated systems "for providing secure data transmission over a data network." (Spec, Abstract.) FIG. 2, reproduced below, illustrates an embodiment where the "security processor 12 communicates with one or more processors 10." (Spec, ¶[0051].) As described in the specification, a "TCP/IP processor (not shown) in processor(s) 10 encapsulates the data into TCP/IP packets. The media access controller provides Layer 2 processing (e.g., Ethernet) to encapsulate the TCP/IP packets into Layer 2("L2") packets." (Spec, ¶[0052].) The header of this Layer 2 packet is referred to as "the inner Ethernet header."

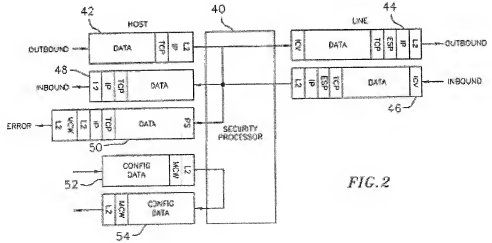


FIG. 2

The processor(s) 10 then "encapsulate the packet of FIG. 1 into another Layer 2 packet for transmission over a Layer 2 link (e.g., link 14) to the security processor 12." (Spec, ¶ [0057].) The header for this second Layer 2 packet is referred to as "the outer Ethernet header." The security processor "recognizes two formats of this custom in-band communication scheme." (Spec., ¶[0061].) "The first format (CLASS-0) is intended for all devices of a company where a flow tag ("FlowID") has been used to identify the unique 'flow' (e.g., secure session) for a packet." (Spec, ¶[0061].) The second format, CLASS-F for FAMILY, "may be used to send configuration packets ***and data packets*** to the security processor." (Spec, ¶[0063].)(emphasis added.)

As further explained in Appellants' specification, the CLASS-F class can be used to communicate data to the security processor for cryptographic processing:

> In some applications, a previously encapsulated packet may be sent to the security processor 810 using the CLASS-FAMILY=security packet type. This packet will be encrypted/authenticated by the security processor 810 using the security association data ("SAData") stored either in local memory or passed in-band with the packet. (Spec, ¶[0135])

Appellants' specification further describes that the inner Ethernet header "may be used to return the packet to the original sender. Thus, the DA [destination address] in the inner Ethernet header may be the address of the Ethernet controller that sent a configuration packet ***or data packet*** to the security processor." (Spec, ¶[0064].)(emphasis added) Thus, "[e]ach device builds the packet that will be sent back to the device." (Spec, ¶[0065].)

The outer Ethernet header includes a destination address, a source address and an Ethernet type field. (Spec, FIG. 3.) The Ethernet type field "may be used to indicate that the packet is associated with a particular entity (e.g., a chip manufacturer) that has registered with

the I.E.E.E." (Spec, ¶ [0057].) For example, a "company such as Broadcom Corporation may have a unique registered Ethernet type 62 that is used to define in-band packet communication." (Spec, ¶[0060].)

The packet generated by the processor further may include a manufacturer-specific header (referred to as the security header). The manufacturer-specific header includes a tag and a type. (Spec, ¶[0059].) The tag may include "FlowID" to "identify the unique 'flow' (e.g., secure session) for a packet." (Spec, ¶[0061].) "The lower 22 bits of the FlowID refer to the location of the security association in memory." (Spec, ¶[0128].) The security processor utilizes the FlowID to obtain the security association.

B. *Independent Claims*

The exemplary support for the subject matter of independent claims 1, 17, 26, and 37 is summarized below.

Claims	Specification Support
1. A method of generating encrypted packets comprising the steps of: receiving, in a security processor, a first Ethernet packet from an originating device, the first Ethernet packet comprising a second Ethernet packet and a memory address associated with a security association, wherein a destination address of the second Ethernet packet is an address of the originating device;	¶¶57-65 ¶¶121-124, 135 ¶¶152, 153, 156-157 FIGs. 2, 3, 9, 18
extracting the memory address and the second Ethernet packet from the first Ethernet packet;	¶¶66, 77, 78 ¶¶125-128, 154,155 FIGs. 9, 18
retrieving the security association from the memory using the received memory address; and	¶¶79, 132, 133, 135 FIGs. 9, 10
encrypting a portion of the extracted second Ethernet packet according to the retrieved security association.	¶¶133, 135 FIG. 9
17. A method of generating encrypted packets by processing at a security processor a first Ethernet packet from an originating device, the first Ethernet packet comprising a second Ethernet packet having a header pre-populated with an address of the originating device as the destination	¶¶57-65, 66, 77, 78 ¶¶121-128, 135 ¶¶152-157

address, and the first Ethernet packet further comprising a memory address associated with a security association, the method comprising the steps of:	FIGs. 2, 3, 9, 18
extracting the memory address and the second Ethernet packet from the first Ethernet packet;	¶¶66, 77, 78 ¶¶125-128, 154,155 FIGs. 9, 18
retrieving the security association from the memory using the extracted memory address;	¶¶79, 132, 133, 135 FIGs. 9, 10
encrypting a portion of the packet data of the extracted second Ethernet packet according to the retrieved security association; and	¶¶133, 135 FIG. 9
returning the second Ethernet packet to the originating device, wherein the returned second Ethernet packet includes the pre-populated header and the encrypted packet data.	¶¶64-65 ¶135
26. A method of generating packets, at an originating device, to be encrypted by a security processor comprising the steps of:	
generating a first Ethernet packet, wherein the first Ethernet packet includes a header having an address of the originating device as the destination address and packet data;	¶¶57-65 ¶¶121-124, 135 ¶¶152, 153, 156-157 FIGs. 2, 3, 9, 18
associating a security association with the first Ethernet packet;	¶¶66, 77, 78, 121 ¶¶125-128, 154,155 FIGs. 9, 18
identifying a memory address associated with the security association; and	¶¶66, 77, 78 ¶¶125-128, 154,155 FIGs. 9, 18
generating a second Ethernet packet encapsulating the memory address and the first Ethernet packet, wherein the second Ethernet packet includes a header having an address of the security processor as the destination address,	¶¶57-65 ¶¶121-124, 135 ¶¶152, 153, 156-157 FIGs. 2, 3, 9, 18
wherein a portion of the packet data of the generated first Ethernet packet is cryptographically processed by the security processor and the portion of the packet data is replaced with the cryptographically processed data when the first Ethernet packet is returned to the originating device.	¶¶64-65 ¶¶133, 135 FIG. 9

37. A security processor for generating encrypted packets by processing a first Ethernet packet received from an originating device, the first Ethernet packet comprising a second Ethernet packet including a header having an address of the originating device as the destination address and a memory address associated with a security association, comprising:	¶¶57-65 ¶¶121-124, 135 ¶¶152, 153, 156-157 ¶¶82-102 FIGs. 1, 4, 18-21
a memory for storing the security association;	¶¶82-102 FIGs. 1, 4, 10
a Gigabit MAC for receiving the first Ethernet packet;	¶¶82-102 FIGs. 1, 4, 5-7
a processor, connected to receive at least a portion of the first Ethernet packet from the Gigabit MAC, for	¶¶82-102 FIG. 1, 2, 4, 5, 10, 12, 13, 18-21
extracting the memory address from the first Ethernet packet; and	¶¶66, 77, 78 ¶¶125-128, 154,155
retrieving the security association from the memory using the extracted memory address; and	¶¶79, 132, 133, 135
an encryption processor, connected to the processor, for encrypting at least a portion of the second Ethernet packet according to the retrieved security association; and	¶¶133, 135 FIG. 1, 2, 4, 5, 10, 12, 13, 18-21
a unit configured to transmit the second Ethernet packet, including the at least a portion encrypted by the encryption processor, to the originating device	¶¶64-65 ¶135 FIG. 1, 2, 4, 5, 10, 12, 13, 18-21

VI. Issues to be Reviewed on Appeal

In the Final Office Action mailed on October 14, 2009, the specification was objected to as failing to provide proper antecedent basis for the claimed subject matter. Claims 1-7, 9, 13-33, and 35-40 were rejected under 35 U.S.C. § 112, first paragraph, for allegedly failing to comply with the written description requirement. Claims 1-7, 9, 13-33, and 35-40 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1-4, and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Bryers *et al*, U.S. Patent Publication 2003/0126233 ("Bryers") in view of Hadzic, U.S. Patent No. 7,130,303 ("Hadzic") further in view of Mercer *et al*, U.S. Patent Publication No. 2003/0018908 ("Mercer"). Claims 5-7 and 9 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Bryers, Hadzic, and Mercer in view of Stevens, *TCP/IP Illustrated* ("Stevens").

1. Whether the Examiner erred in concluding that the specification failed to provide proper antecedent basis for claims 5-7, 9, 18, 30, 35, 36, and 38.

2. Whether the Examiner erred in concluding that claims 1-7, 9, 13-33, and 35-40 are unpatentable under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description.

3. Whether the Examiner erred in concluding that claims 1-7, 9, 13-33, and 35-40 are unpatentable under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to point out and distinctly claim the subject matter which applicant regards as the invention.

4. Whether the Examiner erred in concluding that claims 1-4, and 16[1] are unpatentable under 35 U.S.C. § 103(a) over Bryers in view of Hadzic and Mercer.

5. Whether the Examiner erred in concluding that claims 5-7, 9, 18-21, 30, 32, and 33 are unpatentable under 35 U.S.C. § 103(a) over Bryers, Hadzic, Mercer, in view of Stevens, *TCP/IP Illustrated* ("Stevens").

---

[1] The Final Office Action states that only 1-4 and 16 were rejected by the Examiner. Appellants believe that this was a typographical error. Therefore, in the interest of expediting the proceeding, Appellants are addressing the rejection of claims 1-4, 16, 17, 22-29, 31, and 35-40.

VII. Argument

A. *Objection to Specification and Rejections Under 35 U.S.C. § 112*

The Examiner's Objection to the Specification and Rejections Under 35 U.S.C. § 112 first and second paragraphs derive from the same perceived issues:

1) The specification fails to provide proper antecedent basis for the recitations "a user-specific type field" and "wherein the outer Ethernet header comprises a user-specific type field."

2) The specification fails to provide proper antecedent basis for the recitations of "pre-populated with an address ... " and "the pre-populated header" as recited in claim 17.

Regarding these elements, the Examiner states that "specification fails to provide proper antecedent basis" for these recitations, the claims contain subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that inventors had possession of the claim invention, and as being indefinite because there is "no antecedent basis within the applicant's specification for the language."

USER-SPECIFIC TYPE FIELD

Claims 5-7, 9, 18, and 30 recite a "user-specific [Ethernet] type." Paragraph [0060] of Appellants' specification (as published) recites:

> When the security processor receives a packet 60 with the security processor's address in the DA field of the outer header 66, the security processor may check the Ethernet type field 62 to determine how to process the packet header. A company such as Broadcom Corporation may have a unique registered Ethernet type 62 that is used to define in-band packet communication.

Thus, the specification describes that a user (e.g., "Broadcom") may have a ***unique registered*** Ethernet type 62. That is, this unique registered Ethernet type is user-specific.

In response to Appellants' argument that paragraph 60 provides adequate antecedent basis for the claim recitations, the Examiner stated that "applicant's claims are merely attempting to recite the prior art Ethernet type field while furthermore using terminology that is not found within the applicant's disclosure." (Final Office Action, 12). The Examiner's position is legally incorrect.

As discussed in MPEP 2173.05(e), "[t]he mere fact that a term or phrase used in the claim has no antecedent basis in the specification disclosure does not mean, necessarily that the term or phrase is indefinite. There is no requirement that the words in the claim must match those used in the specification. Applicants are given a great deal of latitude in how they choose to define their invention so long as the terms and phrases used define the invention with a reasonable degree of clarity and precision."

The recitation "user-specific type" and "user-specific Ethernet type" are defined with reasonable clarity and precision in Appellants' specification.

PRE-POPULATION RECITATIONS

The Examiner further takes the position that the specification fails to provide proper antecedent basis for the recitations of "pre-populated with an address ..." and "the pre-populated header" as found recited within claim 17. The Examiner's position is based on a fundamental misunderstanding of Appellants' specification.

In regards to these elements, the Examiner states that

> The examiner notes that the applicant's disclosure appears to provide antecedent basis for two distinct concepts: IPSec communication between hosts on a network (e.g., figs. 4, 9; par. 66, 76-78) and the configuration of a security processor (e.g., par. 63-65). However, the applicant's specification does not support the mixture of security processor configuration and IPSec processing as presently claimed. In other words, a security processor either receives configuration packets, wherein packets may be sent back to a host device or a security processor may receive

> communication packets, wherein the processor performs IPSec processing upon such packets and sends them outbound over a network.

(Final OA, p. 4.) The Examiner is incorrect.

As described in Appellants' specification, the "CLASS-F packet 72 may be used to send configuration packets and ***data packets*** to the security processor." (Spec., ¶[0064].)(emphasis added). The specification explains how the CLASS-F packets, e.g., are populated:

> The inner Ethernet header is a header that may be used to return the packet to the original sender. Thus, the DA in the inner Ethernet header may be the address of an Ethernet controller that sent a configuration packet or data packet to the security processor. This format provides a relatively easy mechanism for supporting multiple devices with a single security processor.
>
> Each device builds the packet that will be sent back to the device. The security processor may then simply strip the outer header and the security header (F, C, MCW), modify the packet data (SAP, MAP, MEP, DATA), if applicable, and send the inner packet back to the device. For example, for a read access, the returned packet would contain the data from the memory or register accessed.

(Spec. ¶¶[0064-65].) Thus, the specification explains that the message originator generates an inner Ethernet packet with its address as the destination address. That is, the header is "pre-populated with an address of the originating device as the destination address."

Appellants' specification further explains that the CLASS-F packets may be encrypted by the security processor:

> In some applications, a previously encapsulated packet may be sent to the security processor 810 using the CLASS-FAMILY=security packet type. This packet will be encrypted/authenticated by the security processor 810 using the security association data ("SAData") stored either in local memory or passed in-band with the packet. This format is required for some Microsoft applications. A SAData.Cap_En bit may be set to zero to prevent the security processor 810 from attempting encapsulation for these types of packets.

(Spec., ¶[0135].) Based on the disclosure of Appellants' specification, a CLASS-F packet may be pre-populated "with an address of the originating device as the destination address" and may further be cryptographically processed as described in paragraph 135.

The recitations "pre-populated with an address ..." and "the pre-populated header" are defined with reasonable clarity and precision in Appellants' specification.

1. Issue 1: The Examiner Erred in Concluding that the specification failed to provide proper antecedent basis for the claimed subject matter.

In the Final Office Action, the specification was "objected to as failing to provide proper antecedent basis for the claimed subject matter." (Final OA, p. 2). The Office Action further stated that the "specification fails to provide proper antecedent basis for the recitations (or essentially similar recitations) 'a user-specific type field,' 'wherein the outer Ethernet header comprises a user-specific type field', as found recited within claims 5-7, 9, 18, 30, 35, 36, and 38[2]" and "fails to provide proper antecedent basis for the recitations of 'pre-populated with an address ...' and 'the pre-populated header' as found recited within claim 17." (Final OA, p. 2.)

As discussed in detail above, the specification provides adequate antecedent basis for these recitations. Therefore, the Examiner's objection to the specification should be withdrawn.

2. Issue 2: The Examiner Erred in Concluding that Claims 1-7, 9, 18, 30, 35, 36, and 38 Were Unpatentable Under 35 U.S.C. § 112, First Paragraph, for Failing to Comply With the Written Description Requirement.

Claims 1-7, 9, 13-33, and 35-40 were rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. Specifically, the Office Action states that the "Applicant has not clearly pointed out where the new (or amended) claim is supported, nor does there appear to be a written description of the claim limitations in the application as filed (see above objection to the specification)." (Final OA, pp. 4-5.) Appellants respectfully disagree.

---

[2] Claims 35, 36, and 38 does not recite a "user-specific type," as indicated by the Examiner.

The fundamental factual inquiry for determining compliance with the written description requirement is "whether the specification conveys with reasonable clarity to those skilled in the art that, as of the filing date sought, applicant was in possession of the invention as now claimed." M.P.E.P. § 2163.02, *citing Vas-Cath, Inc. v. Mahurkar*, 19 U.S.P.Q.2d 1111, 1117 (Fed. Cir. 1991). Possession may be shown by showing that the invention was "ready for patenting," for example, by describing distinguishing identifying characteristics sufficient to show that the applicant was in possession of the claimed invention. M.P.E.P. § 2163.02, *citing Pfaff v. Wells Elecs., Inc.*, 525 U.S. 55, 68 (1998).

The above citations from the specification, among others, demonstrate that the specification describes the claimed invention in sufficient detail that one skilled in the art can reasonably conclude that the inventor had possession of the claimed invention. Accordingly, the Examiner's rejection under 35 U.S.C. § 112, first paragraph should be withdrawn.

3. Issue 3: The Examiner Erred In Concluding Claims 1-7, 9, 13-33, And 35-40 Are Unpatentable Under 35 U.S.C. § 112, Second Paragraph, As Being Indefinite For Failing To Point Out And Distinctly Claim The Subject Matter Which Applicant Regards As The Invention.

Claims 1-7, 9, 13-33 and 35-40 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the examiner stated that "applicant's amendments cause the scope of the claims to become indefinite. The examiner notes that there is no antecedent basis within the applicant's specification for the added recitations." (Final OA, pp. 5-6.)

The second requirement of 35 U.S.C. §112, second paragraph, that "the claims must particularly point out and distinctly define the metes and bounds of the subject matter that will be protected by the patent grant" is "an objective one because it is not dependent on the views of

[the] applicant or any particular individual, but is evaluated in the context of whether the claim is definite - i.e., whether the claim is clear to a hypothetical person possessing the ordinary level of skill in the pertinent art."

As discussed above, the elements of claims 1-7, 9, 13-33, and 35-40 would be clear to a hypothetical person possessing the ordinary level of skill in the pertinent art. Therefore, the Examiner's rejection under 35 U.S.C. § 112, second paragraph should be withdrawn.

B. ***Issue 4: The Examiner Erred In Concluding That Claims 1-4, And 16 Are Unpatentable Under 35 U.S.C. § 103(a) Over Bryers In View Of Hadzic And Mercer .***

Claims 1-4, 16, 17, 22-29, 31, and 35-40 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Bryers *et al.*, U.S. Patent Published Application No. 2003/0126233 ("Bryers"), in view of Hadzic, U.S. Patent No. 7,130,303 ("Hadzic"), and in further view of Mercer *et al.*, U.S. Patent Published Application No. 2003/0018908 ("Mercer"). Appellants respectfully disagree.

The combination of Bryers, Hadzic, and Mercer fails to teach or suggest each and every feature of amended independent claims 1, 17, 26, and 37. As described in Appellants' specification, "[e]ach device builds the packet that will be sent back to the device. The security processor may then simply strip the outer header and the security header (F, C, MCW), modify the packet data (SAP, MAP, MEP, DATA), if applicable, and send the inner packet back to the device." (Specification, ¶ [0065].) "The inner Ethernet header is a header that may be used to return the packet to the original sender." (Specification, ¶ [0064].)

The Examiner acknowledges that Bryers fails "to explicitly recite that one Ethernet packet may comprise another Ethernet packet" but alleges that Hadzic "discloses the practice of generating an Ethernet packet comprising another Ethernet packet for delivery over large distributed systems." (Final OA, p. 8.) Hadzic describes "encapsulating contents of each

original Ethernet packet, which originates in a first Ethernet network of an entity, e.g., an enterprise, a customer, or a network service provider, within another Ethernet packet which is given a source address that identifies the new encapsulating packet as originating at a port of a switch that is located at the interface between the first Ethernet network in which the original Ethernet packet originated and a second Ethernet network, e.g., the metropolitan area Ethernet network, which is to transport the encapsulating packet" to the destination. (Hadzic, 1:44-53.) Thus, Hadzic describes the use of encapsulation for transporting packets from an originating network to a destination network via an intermediate network, such as a metropolitan area Ethernet network.

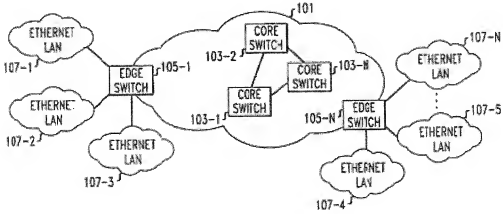
Appellants' claims require more than simple encapsulation. Appellants' claim a specific technique for encapsulation. The Examiner argues that "it may be possible to suggest that the Appellant's recitation of *wherein a destination address of the second Ethernet packet is an address of the originating device* is simply a reference to the fact that an address of a sender may be used by a receiver to send data to the sender." (Final OA, p. 8.)(emphasis in original). Appellants disagree with the Examiner's interpretation.

Appellants' independent claim 1 recites a "first Ethernet packet comprising a second Ethernet packet and a memory address associated with a security association, wherein a destination address of the second Ethernet packet is an address of the originating device." That is, the destination address of the embedded second Ethernet packet is pre-populated by the originating device with the address of the originating device. It is irrelevant that the address of a sender may be used by the recipient to send data to the sender at some time in the future. The relevant inquiry is whether the sender transmits a first Ethernet packet comprising a second

Ethernet packet pre-populated with the destination address of the originating device. Hadzic does not disclose or suggest this element.

FIG. 1 of Hadzic is reproduced below.

FIG. 1



Hadzic addresses problems associated with large tables in Ethernet switches used on a metropolitan scale. As explained in Hadzic:

> However, edge switches 105 of metropolitan Ethernet network 101, are arranged to encapsulate each original Ethernet packet originating in one of LANs 107 into a new Ethernet packet which has a source address that indicates that the new packet originates at a particular port of the one of edge switches 107 that is coupled to the one of LANs 107 in which the original packet originated. (Hadzic, 4:21-27.)
>
> The destination address of the encapsulating packet may be handled in one of several ways. If the one of edge switches 105 which is creating the encapsulating packet is aware of the port of the one of edge switches 105 that serves the destination specified by the packet being encapsulated, then the address of such port is employed as the destination address. However, if the one of edge switches 105 which is creating the encapsulating packet is unaware of the port of the one of edge switches 105 that serves the destination specified by the packet being encapsulated, then it is required that the encapsulating packet reach at least each of edge switches 105 that are serving the entity to which the encapsulating packet is addressed. (Hadzic, 4:32-44.)

Thus, in Hadzic, the destination address of the inner packet is the address of the ultimate message recipient (and not the address of the originating device). The outer packet of Hadzic has a source address of an edge switch associated with the sender and a destination address of an edge switch associated with the recipient.

Thus, Hadzic, like Bryers, does not teach or suggest:

"a first Ethernet packet from an originating device, the first Ethernet packet comprising a second Ethernet packet and a memory address associated with a security association, wherein a destination address of the second Ethernet packet is an address of the originating device," as recited in amended independent claim 1;

"the first Ethernet packet comprising a second Ethernet packet having a header pre-populated with an address of the originating device as the destination address, and the first Ethernet packet further comprising a memory address associated with a security association" and " returning the second Ethernet packet to the originating device, wherein the returned second Ethernet packet includes the pre-populated header and the encrypted packet data," as recited in amended independent claim 17;

"generating a first Ethernet packet, wherein the first Ethernet packet includes a header having an address of the originating device as the destination address and packet data ... generating a second Ethernet packet encapsulating the memory address and the first Ethernet packet, wherein the second Ethernet packet includes a header having an address of the security processor as the destination address, wherein a portion of the packet data of the generated first Ethernet packet is cryptographically processed by the security processor and the portion of the packet data is replaced with the cryptographically processed data when the first Ethernet packet is returned to the originating device," as recited in amended independent claim 26;

and "a first Ethernet packet received from an originating device, the first Ethernet packet comprising a second Ethernet packet including a header having an address of the originating device as the destination address and a memory address associated with a security association" and "a unit configured to transmit the second Ethernet packet, including the at least a portion encrypted by the encryption processor, to the originating device" as recited in amended independent claim 37.

Mercer is directed to a "method for establishing a secure communication channel for information flow between two or more computers communicating via an interconnected computer network." (Mercer, Abstract.) Mercer fails to overcome these deficiencies of Bryers and Hadzic. Accordingly, for at least these reasons, independent claims 1, 17, 26, and 37 are patentable over the combination of Bryers, Hadzic, and Mercer. Claims 2-4 and 16 dependent from independent claim 1; claims 22-25 depend from independent claim 17; claims 27-29, 31, 35, and 36 depend from independent claim 26; and claims 38-40 depend from claim 37. For at least the above reasons, and further in view of their own features, dependent claims 2-4, 16, 22-25, 27-29, 31, 35, 36, and 38-40 are also patentable over the combination of Bryers, Hadzic, and Mercer.

Accordingly, the Examiner's rejection of claims 1-4, 16, 17, 22-29, 31, and 35-40 should be withdrawn.

C. ***Issue 5: The Examiner Erred In Concluding That Claims 5-7, 9, 18-21, 30, 32, and 33 Are Unpatentable Over Bryers, Hadzic, Mercer in further view of Stevens.***

Claims 5-7, 9, 18-21, 30, 32, and 33 were rejected under 35 U.S.C. § 103(as) as allegedly being unpatentable over the combination of Bryers, Hadzic, and Mercer, an in further view of Stevens, *TCP/IP Illustrated* ("Stevens"). Appellants respectfully traverse this rejection.

Claims 5-7 and 9 depend from claim 1; claims 18-21 depend from claim 17; and claims 30, 32, and 33 depend from claim 26. Stevens does not overcome the deficiencies of Bryers, Hadzic, and Mercer relative to amended independent claims 1, 17, and 26 described above. For at least these reasons, and further in view of their own features, dependent claims 5-7, 9, 18-21, 30, 32, and 33 are patentable over the combination of Bryers, Hadzic, Mercer, and Stevens.

Accordingly, the Examiner's rejection of claims 5-7, 9, 18-21, 30, 32, and 33 should be withdrawn.

Conclusion

In view of the foregoing, Appellants respectfully request withdrawal of the Examiner's objection to the specification, the rejection of claims 1-7, 1-7, 9, 13-33, and 35-40 as unpatentable under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description, and the rejection of claims 1-7, 9, 13-33, and 35-40 are unpatentable under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to point out and distinctly claim the subject matter which applicant regards as the invention.

Appellants further request withdrawal of the Examiner's rejection of claims 1-4, 16, 17, 22-29, 31, and 35-40 as unpatentable under 35 U.S.C. § 103(a) over Bryers in view of Hadzic and Mercer and claims 5-7, 9, 18-21, 30, 32, and 33 are unpatentable under 35 U.S.C. § 103(a) over Bryers, Hadzic, Mercer, in view of Stevens.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Lori A. Gordon
Attorney for Third Party Requester
Registration No. 50,633

Date: September 20, 2010

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

1259505_1.DOC

VIII. Claims Appendix

Pursuant to 37 C.F.R. § 41.67(c)(1)(viii), the following is a list of pending claims.

1. (previously presented) A method of generating encrypted packets comprising the steps of:

receiving, in a security processor, a first Ethernet packet from an originating device, the first Ethernet packet comprising a second Ethernet packet and a memory address associated with a security association, wherein a destination address of the second Ethernet packet is an address of the originating device;

extracting the memory address and the second Ethernet packet from the first Ethernet packet;

retrieving the security association from the memory using the received memory address; and

encrypting a portion of the extracted second Ethernet packet according to the retrieved security association.

2. (previously presented) The method of claim 1 wherein the first Ethernet packet also includes outer Ethernet header and a manufacturer header.

3. (previously presented) The method of claim 2 wherein the manufacturer header includes the memory address.

4. (previously presented) The method of claim 3 wherein the outer Ethernet header comprises an Ethernet address of the security processor.

5. (previously presented) The method of claim 4 wherein the outer Ethernet header comprises a user-specific type.

6. (previously presented) The method of claim 5 wherein a first byte of the manufacturer header is set to zero.

7. (previously presented) The method of claim 6 wherein a portion of the manufacturer header following the first byte of the manufacturer header includes the memory address.

8. (canceled)

9. (previously presented) The method of claim 1 wherein the extracting step comprises determining whether an Ethernet type field from the first Ethernet packet comprises a user-specific Ethernet type.

10-12. (canceled)

13. (previously presented) The method of claim 1 wherein the retrieving step comprises retrieving the at least one security association from a memory in the security processor.

14. (previously presented) The method of claim 1 wherein the encrypting step comprises using an encryption key associated with the security association.

15. (previously presented) The method of claim 1 wherein the encrypting step comprises using an encryption algorithm defined by the security association.

16. (previously presented) The method of claim 1 wherein the extracting step comprises determining whether an Ethernet address from the first Ethernet packet matches an Ethernet address of the security processor.

17. (previously presented) A method of generating encrypted packets by processing at a security processor a first Ethernet packet from an originating device, the first Ethernet packet comprising a second Ethernet packet having a header pre-populated with an address of the originating device as the destination address, and the first Ethernet packet further comprising a memory address associated with a security association, the method comprising the steps of:

extracting the memory address and the second Ethernet packet from the first Ethernet packet;

retrieving the security association from the memory using the extracted memory address;

encrypting a portion of the packet data of the extracted second Ethernet packet according to the retrieved security association; and

returning the second Ethernet packet to the originating device, wherein the returned second Ethernet packet includes the pre-populated header and the encrypted packet data.

18. (previously presented) The method of claim 17 wherein the extracting step comprises determining whether an Ethernet type field from the first Ethernet packet comprises a user-specific Ethernet type.

19. (previously presented) The method of claim 17 wherein the extracting step comprises determining whether a first byte following an Ethernet type field from the first Ethernet packet is set to a zero.

20. (previously presented) The method of claim 17 wherein the extracting step comprises extracting an address from second, third and fourth bytes following an Ethernet type field from the first Ethernet packet.

21. (previously presented) The method of claim 17 wherein the extracting step comprises extracting an address from a lower 22 bits of second, third and fourth bytes following an Ethernet type field from the first Ethernet packet.

22. (previously presented) The method of claim 17 wherein the retrieving step comprises retrieving the security association from a memory in a security processor.

23. (previously presented) The method of claim 17 wherein the encrypting step comprises using an encryption key associated with the security association.

24. (previously presented) The method of claim 17 wherein the encrypting step comprises using an encryption algorithm defined by the security association.

25. (previously presented) The method of claim 17 wherein the extracting step comprises determining whether an Ethernet address from the first Ethernet packet matches an Ethernet address of a security processor.

26. (previously presented) A method of generating packets, at an originating device, to be encrypted by a security processor comprising the steps of:

generating a first Ethernet packet, wherein the first Ethernet packet includes a header having an address of the originating device as the destination address and packet data;

associating a security association with the first Ethernet packet;

identifying a memory address associated with the security association; and

generating a second Ethernet packet encapsulating the memory address and the first Ethernet packet, wherein the second Ethernet packet includes a header having an address of the security processor as the destination address,

wherein a portion of the packet data of the generated first Ethernet packet is cryptographically processed by the security processor and the portion of the packet data is replaced with the cryptographically processed data when the first Ethernet packet is returned to the originating device.

27. (previously presented) The method of claim 26 wherein the generating a second Ethernet packet comprises generating an outer Ethernet header comprising an address of a security processor.

28. (previously presented) The method of claim 26 wherein the generating a second Ethernet packet comprises generating an outer Ethernet header and a manufacturer header.

29. (original) The method of claim 28 wherein the outer Ethernet header comprises an Ethernet address of a security processor.

30. (previously presented) The method of claim 28 wherein the outer Ethernet header comprises a user-specified Ethernet type.

31. (previously presented) The method of claim 28 wherein the manufacturer header comprises the memory address.

32. (previously presented) The method of claim 28 wherein a first byte of the manufacturer header is set to zero.

33. (previously presented) The method of claim 28 wherein second, third and fourth bytes of the manufacturer header comprise the memory address.

34. (canceled)

35. (previously presented) The method of claim 26 further comprising the steps of:

receiving data to be sent over an Ethernet network; and

incorporating the data into the first Ethernet packet.

36. (previously presented) The method of claim 26 further comprising the step of transmitting the second Ethernet packet to at least one security processor.

37. (previously presented) A security processor for generating encrypted packets by processing a first Ethernet packet received from an originating device, the first Ethernet packet comprising a second Ethernet packet including a header having an address of the originating device as the destination address and a memory address associated with a security association, comprising:

a memory for storing the security association;

a Gigabit MAC for receiving the first Ethernet packet;

a processor, connected to receive at least a portion of the first Ethernet packet from the Gigabit MAC, for

extracting the memory address from the first Ethernet packet; and

retrieving the security association from the memory using the extracted memory address; and

an encryption processor, connected to the processor, for encrypting at least a portion of the second Ethernet packet according to the retrieved security association; and

a unit configured to transmit the second Ethernet packet, including the at least a portion encrypted by the encryption processor, to the originating device.

38. (previously presented) The security processor of claim 37 wherein the first Ethernet packet comprises an outer Ethernet header and a manufacturer header including the memory address.

39. (previously presented) The security processor of claim 37 wherein the encryption processor comprises a IPsec processor.

40. (original) The security processor of claim 37 wherein the security processor is an integrated circuit.

41-53. (canceled)

IX. Evidence Appendix

None.

X. Related Proceedings Appendix

None.